The evolution of safety practice in railway signalling

Prepared on behalf of the IRSE International Technical Committee
by Yuji Hirao

The purpose of the IRSE's International Technical Committee (ITC) is to provide thought leadership and disseminate learning on technical topics relevant to train control and communication systems. This provides value not only to IRSE members but also to the wider rail industry. The committee's particular strength lies in its international membership, enabling engineering principles and practices from a diverse range of countries to be brought to bear upon the subjects that are debated.

In this report Yuji Hirao describes the way in which safety practice has developed, and draws some comparisons between signalling and other industries.

Introduction

In the long history of railway signalling, its unique safety technologies have continuously evolved on the basis of the lessons learned from accidents. When microelectronics and computers were applied to railway signalling during the 1980s, many detailed, in-depth studies were carried out on the basis of conventional safety practices based on a fail-safe philosophy, which were all rather qualitative and deterministic. Later a risk-based approach which deals with probability of hazardous failure was introduced, and although the importance of fail-safe as best practice has not changed, there is nowadays a tendency that the quantitative approach, based on hazardous failure probability, has more importance and relevance than the qualitative and deterministic one. Is this the direction we should be taking, particularly in view of the coming generation change of new signal engineers with much more of an IT background? We should be thinking how safety is determined and managed within the context of railway signalling.

Current practice and safety technologies in railway signalling

Fail-safe

In discussing safety, whether or not a safe state can be defined is an important question. In the case of railways, the stoppage of trains is, in general, the safest result when malfunction of relevant systems or any other difficulties occur, i.e. fail-safe. This is a specific feature of railway signalling as well as the rationale for how safety is managed. The aim of fail-safe design is to achieve the required safety enhancement at a comparatively low cost, although, as a trade-off, system reliability is very often reduced because of the restrictive result of a fail-safe configuration.

Safety technologies for computerised railway signalling are now well described in the standard EN 50129 [1], where safety technologies are categorised into three areas: composite fail-safe, reactive fail-safe and inherent fail-safe.

The basic idea of the composite and reactive fail-safe categories is fault detection and negation as illustrated in figure 1. In the case of composite fail-safe, fault detection is performed by comparison of the same items, and the 2oo2 (two out of two) or 2oo3 (two out of three) configurations are normally

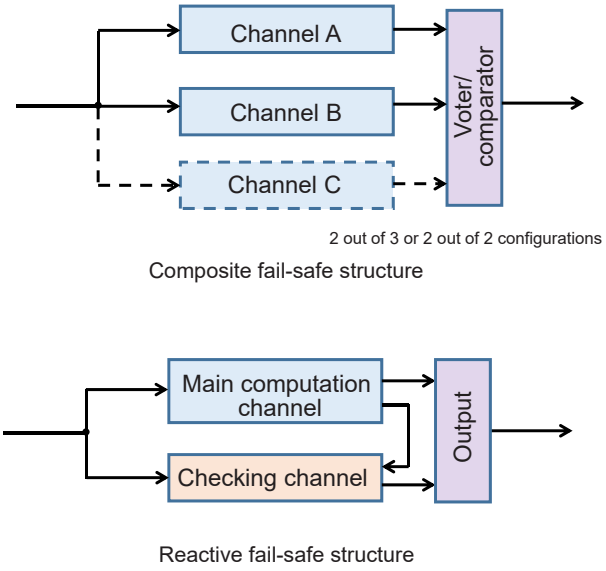

Figure 1 – Principles of composite and reactive fail-safe.

adopted. Reactive fail-safe performs fault detection by applying diversification, for example, by using two different software configurations on either one central processing unit (CPU) or two different CPUs. This enables the system outputs to be compared for integrity. On the other hand, inherent fail-safe is realised by the characteristics of a single item of which the failure modes do not create dangerous situations, and failure mode catalogues (of items which should be considered for inherent fail-safe) are provided in an Annex to the standard.

When microcomputers were introduced in mid 1980s, diagnostic functions became the main force of the CPUs, as composite and reactive functions are realised by CPUs. However, the importance of the inherent fail-safe has not changed because the output must be fixed to a safe state in a fail-safe manner if any malfunction occurs. This also indicates that reliability is an important part of achieving safety, but will not in itself guarantee sufficient safety conditions.

Influence of risk-based functional safety on railway signalling

The UIC A118 committee contributed greatly to the introduction of microcomputers into railway signalling from the mid-1970s to the mid-1980s. At that time, safety measures were discussed in a qualitative/deterministic way, though the need for a risk-based/quantitative approach was recognised and gradually introduced.

In EN 50129, the overall safety level is evaluated by comparing the tolerable risk (and a typical reference value is 10^{-9} per hour per safety function). Although inherent fail-safe is important as mentioned above, this may cause over-reliance on quantitative evaluation and underestimation of best practice, i.e., a conventional safety approach. Particularly in the case of software-based systems, we should know that quantitative values are only one aspect of evaluation/validation. We must also

remember that lessons should be learned from the misuse of SIL [2] and that safety has to be considered from many different angles. The UK Ladbroke Grove rail accident in 1999 revealed shortcomings in driver training, signal sighting, flank protection, as well as the absence of a complete and effective ATP system. This emphasizes the importance of using a holistic risk based approach for all operational aspects of running a railway.

Situations apart from railway signalling and their safety technologies

New analysis and description methods of safety functions

For further understanding of the distinct features of railway signalling safety when considering the direction to proceed, a comparison with other well-advanced industrial practices is useful. In the field of safety-critical complex systems, e.g., in aerospace technology, systems are correlated with each other (i.e., into a system of systems), and it is far from simple to identify hazards and to decide system safety requirements.

Conventional hazard analysis methods like FTA (Fault Tree Analysis) are not necessarily available to timing-related phenomena, and a new methodology, STAMP/STPA (Systems Theoretic Accident Model and Processes / System-Theoretic Process Analysis) has been proposed [3]. In STAMP/STPA, hazard analyses are carried out on the basis of four timing-related control actions, which have been experientially obtained through investigations into a huge number of accidents so as to establish a range of accident scenarios, e.g. "control actions stopped too soon or applied too long".Safety countermeasures are set up against the causes of the scenarios.

GSN (Goal Structuring Notation), which is a graphical notation that aims to document explicitly the individual elements of any argument (claims, evidence and contextual information), has been discussed among software researchers who are interested in safety-critical systems, to clearly define safety requirements and to produce proper safety cases [4][5]. If safety requirements based on GSN could be correctly related to model-based software development, confidence in software would be increased.

In the military, a document known as MIL-STD 882E from the US Department of Defense [6] which has been revised by adding software aspects, prescribes software assessments and their consequent level-of-rigour tasks, introducing software control categories and their software safety criticality matrix. MIL-STD 882E requires, as a precondition of the software development, rigorous functional hazard analysis (FHA) against potential hazards to define its safety requirements.

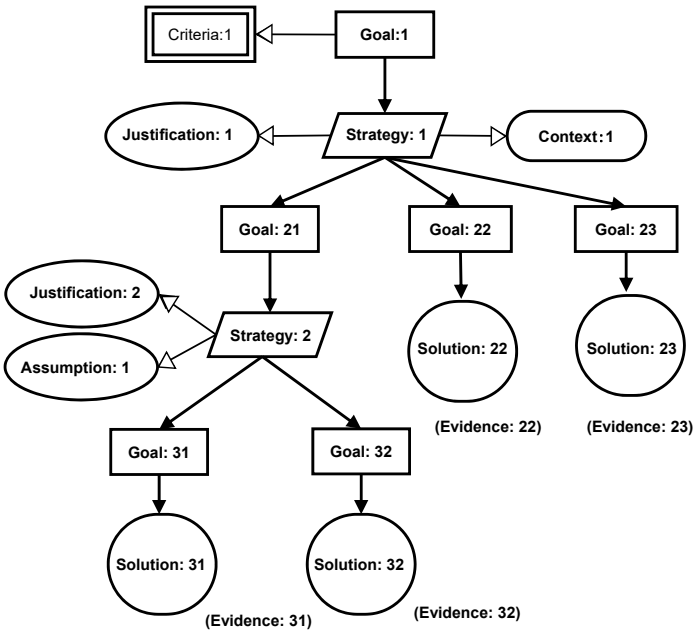

Figure 2 – Principal elements of Goal Structuring Notation.

Validation tool for machinery safety

The experience of safety technologies in other industries offers useful material for consideration. Similar to the case of railway signalling, the safe state in machinery safety can be clearly defined, i.e. bring the process to a stop, though the target safety levels are different. Categories, which are defined in ISO 13849-1 [7] as the classification of machinery safety systems in respect to the minimisation of faults and their subsequent behaviour should a fault occur, are similar to the fail-safe concept in railway signalling. These categories are achieved by the structural arrangement of the parts, fault detection and/or by their reliability.

Specifically, inherent safety design measures are achieved by avoiding hazards or reducing risks by a suitable choice of design features for the machine and/or for the interaction between the exposed persons and the machine, and these design measures are part of the safety principles. For electric/electronic control (i.e., functional safety), more concrete information regarding these safety principles as well as descriptions of well-tried components, are also provided as informative validation tools in ISO 13849-2 [8]. In reality, the laying down of safety principles and use of tried and tested components are well described and understood and are factors also applicable to railway signalling.

Relevance to railway signalling

Robots, in particular personal care robots that provide human physical contact applications to improve the quality of life of intended users irrespective of age or capability, and road vehicle self-driving technologies have made enormous progress recently, attracting wide social interest. These have been developed considering IEC 61508 (functional safety) [9] and its derivative standards, which predominantly relies on quantitative analyses.

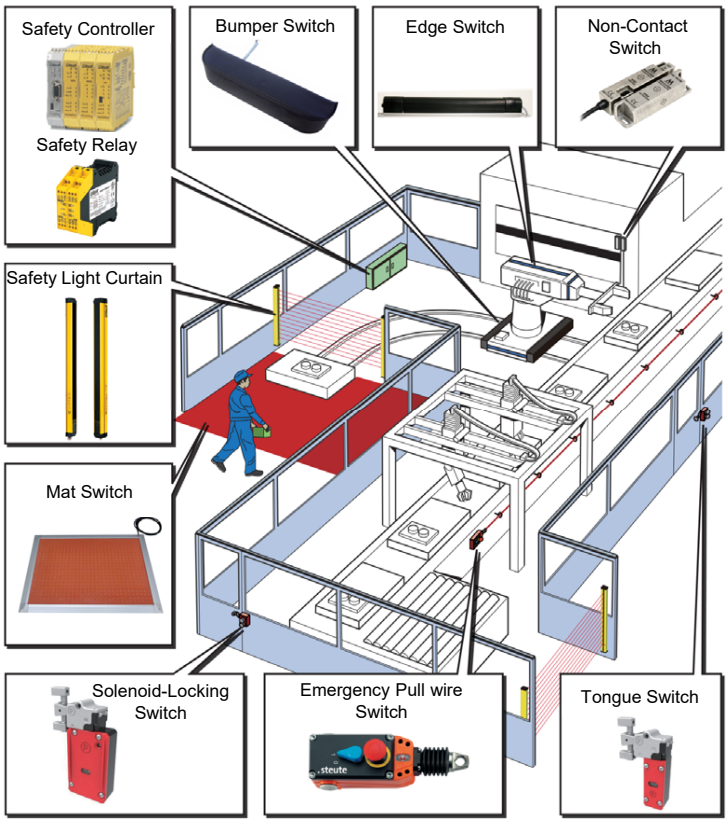

Figure 3 – Examples of machinery safety systems. *Figure Azbil Trading.*

The trend of the above-mentioned new methods should be recognised and interpreted in a way that would be applicable for railway signalling systems, whereby safety should be considered from many different angles, not only relying on the quantitative but also on a deterministic approach. Although the concept of a fail-safe philosophy should continue to be developed in the future to the extent that a safe transportation service can be ensured even in the case of malfunction of the signalling systems, we should first understand the importance of our evolving practice and produce the mechanisms which ensure ever greater safety. This is demonstrated and justified by the following.

Future directions of best practice in railway signalling safety technologies

UIC project: the use of signalling relays

A UIC signalling expert group is now finalising the four-year project, "*The Use of Signalling Relays*", of which the major deliverable is a technical paper of over 170 pages. The development and application of signalling relays is a good example of the spread of best practice in railway signalling. Despite the introduction of computers, relays will never be obsolete, and it is significant that the project has considered afresh the use of relays from both a quantitative and deterministic view, thus demonstrating the value of an alternative approach [10].

This project, however, has revealed that for some specific older technologies, the documentation, including the knowledge of the experts at the time, is either non-existent or even if it does exist, the rationale or theoretical background is not commensurate with modern day safety practice. It is also clear that new computerised systems need to interface with legacy systems because railway signalling systems are rarely implemented as a totality and therefore precise understanding and knowledge of legacy systems has to be part of the overall safety assurance.

The UIC project has revealed that safety best practice, especially for existing elements of railway signalling is already insufficiently controlled and documented. This should be a warning to us all, and more effort needs to be expended to right this deficiency.

Security

Recent sophisticated signalling systems, including radio-based train control systems, are connected to communication networks (also often radio based), and nowadays the security of these is even more important [11]. Recent worldwide cyber attacks on healthcare administrative systems have demonstrated the necessity to have in place effective counter measures that will enable systems to be resilient.

Safety and security have one strong similarity and one major difference. As for the similarity, risk assessment is necessary for both safety and security, meaning that a hazard/threat analysis has to be carried out. This relates primarily to safety aspects where a deterministic approach and use of traditional safety practices lead to a quantitative analysis from which the priorities can be ascertained. However, it is evident that the risks associated with security are more difficult to assess since signal engineers do not have the necessary experience when compared with safety practice, and moreover the hazards themselves evolve and are constantly changing. This aspect is thus fundamentally different.

The development of best practice for security is an urgent task, and this must be a continuing process as new technologies which are applicable to railway signalling are invented and developed. It is vital that signal engineers work with other safety critical industries to study the threats and safeguards that will be needed to ensure safe and reliable use of new technology, putting priority on mechanisms and theory rather than probability.

Conclusion

The most important of the distinct features of railway signalling is, as discussed above, fail-safe, and this has not changed even after risk-based functional safety has been broadly introduced into railways and industries. In order to realise sophisticated railway signalling systems which enhance railway traffic service quality, we need to learn the cutting-edge technologies which are developing rapidly in academia and advanced new industries, and to introduce them into railways, never forgetting the distinct features of railway signalling.

References

[1] CENELEC EN50129:2003, "Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling", May 2013, 1. Also published as IEC 62425:2007.

[2] Muttram R, Kessel C, on behalf of the IRSE International Technical Committee, "Understanding SIL", IRSE News, October 2015.

[3] Leveson N G, "Engineering a Safer World: Systems Thinking Applied to Safety", The MIT Press, ISBN-13: 9780471846802 - January 2012.

[4] Kelly T P, Weaver R A, "The Goal Structuring Notation - A Safety Argument Notation", Proceedings of the Dependable Systems and Networks 2004 Workshop on Assurance Cases, July 2004.

[5] Mizumoto K, Hirao Y, "An Evaluation Method of GSN Safety Argument Development and its Application to Railway Signalling Systems", ASPECT, November 2017.

[6] MIL-STD-882E "Department of Defense Standard Practice – System Safety", 11 May 2012.

[7] ISO 13849-1:2015 "Safety of machinery – Safety-related parts of control systems – Part 1 General principles for design", 2015, 3.

[8] ISO 13849-2:2012 "Safety of machinery – Safety-related parts of control systems – Part 2 Validation", 2015, 2.

[9] IEC 61508:2010 "Functional safety of electrical/electronic/programmable electronic safety-related systems" 2010, 2.

[10] Schulz J, Sorsimo T, "Maintaining knowledge about the use of signalling relays", ASPECT, November 2017.

[11] Howe N, on behalf of the IRSE International Technical Committee "Cybersecurity in railway signalling systems", IRSE News, September 2017.

References [5] and [10] are papers to be presented at the IRSE ASPECT 2017 Conference in Singapore next month, and will be available on the IRSE web site after the conference.